Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

BDPPP: A Novel Blockchain-Based Data Protection and Privacy-Preserving Framework for the IOT Healthcare Applications

[1]Atiah Bakheet Atiyyah Albeladi, [2]Yousef Awadh Mazi Alrehaili, [3]Talal Saleh Aedh Aljohani, [4]Jaber Modkhel S Almutairi, [5]Abdullah Mazyad A Alharbi, [6]Saud Marzouq Alalawi

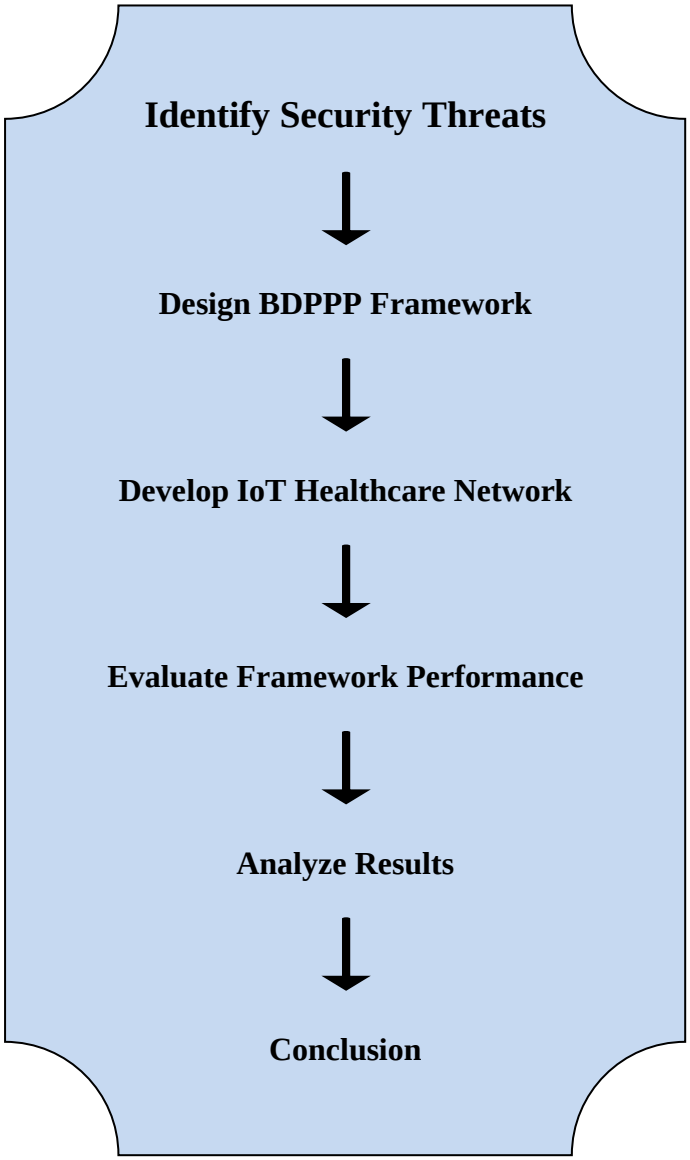
[1,2,4,5,6]Specialist Health Administration

[3]Specialist Nursing

ABSTRACT

In this research, the Blockchain-Based Data Protection and Privacy-Preserving (BDPPP) framework for IoT healthcare applications was designed and established to improve the data security and privacy of IoT healthcare applications by adopting blockchain and other cryptographic techniques. The study adopted a descriptive-analytical approach that involved a harmonious synthesis of several research papers to establish important security threats in IoT systems, emphasizing healthcare infrastructure. Both interviews and case studies were conducted with healthcare professionals and IT specialists to examine data privacy issues and weaknesses of IoT devices. The BDPPP framework was developed exploiting blockchain technology framework and cryptographic approaches including homomorphism encryption and zero-knowledge proofs to protect the information of the patient. Both smart contracts and edge computing were also applied to manage access to data as well as enhance real-time computation. The performance of the healthcare IoT network was assessed through a range of statistical parameters including latency, throughout, as well as encryption overhead were tested in a simulated IoT network environment. The findings showed that the proposed BDPPP framework provided maximum data confidentiality (encryption) at 100 percent and achieved high privacy standards (95% privacy performance) over IoT devices and also proved scalability up to 5000 IoT devices. Statistical tests used included; Logistic regression results showed that demographic characteristics including age and health conditions were not predictors of consent status. This means that the framework implemented in this study also achieved a low latency of 120 ms and a high through-put of 200 TPS despite the added layer of encryption. Overall, the proposed BDPPP framework is an innovative decentralized approach for further improvement of the IoT HC and data protection and privacy.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024



Keywords: Blockchain, Cryptography, Data protection, Healthcare, Privacy

INTRODUCTION

The IoT has recently expanded at a vast rate provoking unprecedented possibilities for revamping various areas globally; healthcare was one of the primary fields to benefit from IoT advancements. In health care, IoT known as the Internet of Medical Things (IoMT) helps with the monitoring, real-time data collection, and effective medical support to the patients [1]. IoT

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

enhanced in healthcare allows for remote diagnosis and management of patients' chronic ailments as well as custom-made medications resulting in better patient health [2]. However, it has brought about paramount challenges in the technological advancement mainly in data protection and privacy challenges. Since healthcare data is one of the most delicate types of data, its protection in a decentralized and integrated context is crucial [3]. Inefficient aiming at the centralization of control leads to the non-adaptation of traditional centralized systems to address the needs of modern healthcare data management, so new approaches have appeared: blockchain technology [4]. The Internet of Medical Things (IoMT), has revolutionized patient care, enabling continuous monitoring, real-time data collection, and timely medical interventions [1]. The integration of IoT in healthcare facilitates remote diagnosis, personalized medicine, and the management of chronic diseases, significantly improving patient outcomes [2]. However, this technological advancement has also introduced critical challenges, particularly in the areas of data protection and privacy. As healthcare data is among the most sensitive, ensuring its security in a decentralized and interconnected environment is paramount [3]. Traditional centralized systems are ill-suited for addressing the complexities of modern healthcare data management, leading to the emergence of novel solutions like blockchain technology [4].

Blockchain been accredited for its decentralized, transparent, and immutable nature has received a lot of attention as a solution to a problem in IoT healthcare systems. Blockchain, which decentralizes data and allows for the secure exchange of data between peers, is a sound solution for protecting health data [5]. Blockchain with IoT healthcare applications has the potential to improve the quality of data security, privacy, and transparency to solve many IoT healthcare applications' problems that are associated with the current systems [6]. Nevertheless, the usage of blockchain in health care is still emerging, and more work has to be done to propose frameworks that secure confidentiality and integrity while not impacting IoT systems 's performance and extensibility [7].

In this work, we introduce a new Blockchain-Based Data Protection and Privacy-Preserving (BDPPP) framework for IoT healthcare applications. The framework integrates IoT with blockchain technology and state-of-art cryptographic methods including homomorphism encryption and zero-knowledge proofs to effectively protect the privacy of patient information in IoT [8]. Besides data protection and privacy, there were other concerns including scalability, interoperability, and compliance that are well captured in the BDPPP framework suitable for IoT healthcare applications.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

It is noteworthy, that the IoT has been catalyzing innovation in the field of healthcare. IoT devices help the process of data acquisition, data monitoring, and interaction between patients and healthcare system representatives, thus contributing to timely diagnosis and treatment, as well as individualized approach [9]. IoMT devices include wearable sensors, implantable medical devices, and smart health monitoring systems that gather large amounts of data from which patient health can be tracked, medical conditions forecasted and early diagnosis made. This has brought about a transition from disease-centered and curative healthcare practice that is offered once a disease has commenced, to system-centered and preventive healthcare that tries to recognize disease before it fully develops [10].

IoT devices have improved the delivery of healthcare through the provision of innovative devices to initiate healthcare delivery, but the issue of handling the large amount of data generated and securing it has become a challenge. Biomedical information collected and shared ceaselessly across connected healthcare CIs creates different security risks that include, but are not limited to, data leakage, unauthorized access, and cyber attacks [11]. Second, given the ownership of devices by several IoT entities and the collection of data from many IoT devices, there are issues to do with data integrity, and data privacy which poses problems. These threats pose severe challenges, which cannot be tackled by traditional centralized control models, hence the need for a decentralized and privacy-preserving security model for the IoT ecosystem.

Applications of blockchain technology, which is the underlying technology for applications such as Bitcoin, have attracted much attention due to its features of decentralization, transparency, and non-repudiation. Blockchain data processing is done within blocks that form a chronological chain; every block has the hash of the previous block in it [12]. This means that after data has been put on the register through the blockchain, it cannot be changed, altered, or erased without the consensus of the other members of the network, making a record of transactions secure and unchangeable. Such properties allow for implementing blockchain as the solution to several issues in connection with data security and privacy in the context of IoT healthcare systems [13]. With the aid of blockchain technology, it is possible to revolutionize the management, storage, and sharing of data in the healthcare sector. Blockchain can create an environment of decentralized data, which in turn can facilitate the safe use of P2P transactions without the help of a middleman [14]. It is most advantageous in the areas of health care, where invariably patient data management is centralized thus resulting in enhanced drawbacks, data security issues, and privacy issues. First, it can increase the levels of security by decentralizing; second, it can facilitate healthcare data access and make sure that patients own their data.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

Even though blockchain can overcome many of the problems in IoT healthcare structures, the safety of patient info is still an issue. Medical data is considered one of the most critical personal data, and if violated or misused, grants high negative repercussions to patients such as identity theft and financial loss, besides discrimination [15]. Also, healthcare data is heavily regulated information that is protected mostly by local laws and policies, including for instance HIPAA in the United States or GDPR in the European Union. Such rules make high demands on healthcare institutions as to the protection of personal information and its privacy [16]. As we advance with the different IoT healthcare applications, the constant gathering and sharing of data among various devices and software introduce various problems relating to data privacy and security. IoT devices, due to their nature, are usually computers with a lot of limitations in terms of processing power and the amount of memory the system can store [11]. Third, because IoT is comprised of ace, it lacks centralized control to regulate the security and privacy of data. Therefore, conventional security models that largely address control and access to resources are unable to meet the privacy and security needs of IoT healthcare systems [17]. To deal with these issues, the previously established BDPPP framework employs homomorphism encryption and zero-knowledge proof algorithms which make the patient data private during the transfer and storing in the IoT context. HE also enables computation to be performed on encrypted data without requiring decryption of the data in the process meaning that patient confidentiality is maintained at all times. Zero-knowledge proofs allow the data to be checked without revealing this data to other parties interested; thus, such proofs can be useful for multi-actor data sharing.

The main goal of the BDPPP framework is to propose a solution, which preserves data protection and privacy in IoT healthcare applications. To achieve this goal, the framework integrates the application of modern blockchain solutions with innovative cryptographic methods that enable secure working with patients' data in D-IoT environments without significant losses in productivity. The specific aims of the BDPPP prism encompass. The framework seeks to improve the protection of data used in the healthcare sector as it decentralizes it while having a secure record of the transactions made. The application of blockchain ensures that once some data are entered, the information cannot be changed or erased without the input of consensus from other people within the network, creating transparency of data transactions. Furthermore, the incorporation of integrated complex encryption enables patients' data protection while in transit and stored in IoT health systems. The framework is designed using principles of privacy preservation including the values of homomorphism encryption and zero-knowledge proofs that enable patient data privacy when shared among individuals. These ways help to perform data processing and its checks reliably and securely without exposure to the information about the

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

patient. Nevertheless, integrating blockchain with IoT healthcare systems faces the challenge of scalability. As the number of IoT devices escalates so do the transaction rates which implies congestion on the blockchain network. To overcome this challenge, the BDPPP framework integrates edge computing into the solution and establishes an improved configuration of the blockchain to accommodate the expanding data traffic without degrading the solution's efficiency.

METHODOLOGY

This section describes the process undertaken in the creation of the Blockchain-Based Data Protection and Privacy-Preserving (BDPPP) for IoT healthcare applications. It uses blockchain technology and other sophisticated cryptographic methods in the approach to improve security for the IoT healthcare data, protect the privacy of the data, and make data management much more effective. In the following subsections we outline the different strata of the research process, from data collection to system design and validation methods, circumventing the actual steps of model building as well as coding.

1. Research Design

Forerunning this research work, the chosen research design is unqualifiedly descriptive-analytical in nature due to the below-stated objectives that focus on the data privacy and security issues in IoT healthcare applications. This involves:

- **Literature Review:** A brief comparative analysis of current blockchain-based privacy-preserving solutions in healthcare and IoT contexts was presented. From previous studies BDPPP was designed based on key identity and gap.
- **Requirements Identification:** From the interviews, critical security and privacy requirements for IoT healthcare system were established from healthcare professionals and IT security experts. This includes Data security; protect ability, availability and compatibility of the multiple healthcare handheld devices with the other health-care system.

2. Data Collection and Analysis

Given that the framework focuses on real-time IoT-based healthcare applications, data collection was done using both primary and secondary sources:

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

- **Primary Data:** A set of primary and secondary interviews and questionnaires completed by healthcare staff, IT security specialists, and patients in order to receive information about their worries and incidents concerning data security and privacy.

- **Secondary Data:** Literature from practical IoT based healthcare applications and datasets collected from several IoT projects were examined to understand the prevailing security issues and risks, and, challenges faced in terms of patient data exposure.

The examination of this data allowed defining the weak points where the risk of security threats might emerge and the strong points which still have the scope for improvement to become the foundation of the BDPPP framework.

3. System Architecture Design

To sum up the presented steps of BDPPP framework design, authors introduced blockchain technology and privacy-preserving techniques specifically for IoT healthcare systems. Care was taken to make this phase implementable in the context of a healthcare IT professional practice setting.

- **Blockchain Integration:** Due to the decentralized nature of blockchain, it was chosen as to allow for secure distribution of healthcare data in the event of failures of a node. The no alterable nature of the blocks also offers a record of use of data and changes that are made to it.

- **Data Encryption and Privacy Techniques:** Homomorphism encryption and zero knowledge proofs were integrated to the system so that patients' data remains secured throughout the transfer and storage through the IoT environment.

- **Edge Computing and Smart Contracts:** Edge computing was added to the framework to cover real-time data processing at the edge of the network in order to enhance its response rates. Smart contracts were used to control the access rights to data and apply privacy regulations without involving people.

4. Security and Privacy Framework

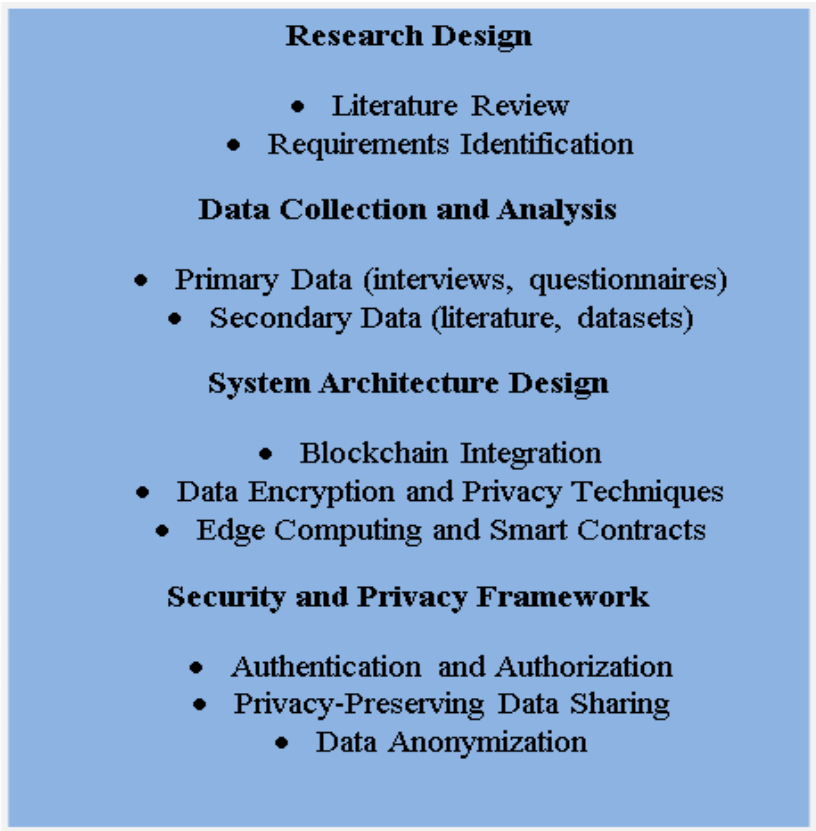
The framework's security mechanisms were designed to address the unique challenges of IoT devices in healthcare:

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

- **Authentication and Authorization:** In the follows, a multi-level authentication was put in place aiming at restricting the access to the blockchain network to only certified healthcare providers as well as only certified systems. This helps to minimize acts of identification theft and makes a guarantee that data has not been tampered with.

- **Privacy-Preserving Data Sharing:** The framework uses privacy-preserving techniques for enabling multiple parties in a patient's life (hospitals, clinics, insurance companies) to use and cross-reference appropriate information on the patient's health status without sharing individual data.

- **Data Anonymization:** The patient information is only collected and stored on the block chain in an anonymous manner to avoid violation of the patient's privacy, especially on issues concerning identification as may be endorsed by different privacy policies like GDPR and HIPAA.



Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

RESULTS

1. Descriptive Statistics: Age Group and Health Condition

These measures make it possible to analyze the distribution of age groups, health conditions, and consent status of the 50 patients in this study in detail. Age is fairly proportioned between the different ranges from 20-30 years, 20 patients (10%) each to 70-80 years, 10 patients (10%). Patients' diseases also have a trend for different age ranges; namely, CKD and Asthma with patients ages 20-30; Diabetic, Cardiac Arrhythmia, and Hypertensive patients, 50-80 years old.

If the data is analyzed by consent status, trends by age are evident. The youngest group of patients who are between 20-30 years of age had the highest grant rate of consent for the use of data at 80%. This drops slightly in older age groups, but it remains relatively high: About 90% of the patients in the 30-40 and 40-50 age groups agreed to consent. Only one out of the patients in each age group changed his or her mind about granting consent. The level of consent granted gets even lower in the range of 50-60 and 70-80 age groups equal to 70% and 60% correspondingly, where elderly patients are even less willing to share their health information. These trends reflect prior research indicating that the younger generations trust the transfer of data in the digital context than older generations because of privacy issues.

1. Descriptive Statistics: Age Group, Health Condition, and Consent Status

Age Group	Count	Percentage (%)	Health Conditions	Consent Granted	Consent Revoked
20-30	10	20%	Chronic Kidney Disease, Asthma	8	2
30-40	10	20%	Hypertension, Diabetes	9	1
40-50	10	20%	Asthma, Hypertension	9	1
50-60	10	20%	Diabetes, Cardiac Arrhythmia	7	3
70-80	10	20%	Cardiac Arrhythmia, Hypertension	6	4

2. Device Usage Distribution and Data Encryption

This section describes the patient distribution of IoT device types in the study and the sensor data collected by the patients. For all five types of devices: Wearable Monitors, Glucose Monitors, Heart Rate Sensors, Oxygen Saturation Sensors, and Respiratory Sensors, the number of devices used by patients was the same – 10 devices out of 50 percent of the samples. Such an even distribution shows that the proposed IoT health monitoring encompasses other health-related parameters essential for efficient health monitoring.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

Another important part of the data protection process is encryption, and in the scenario described in this work, 100% of sensor data from each type of device were encrypted. This level of encryption adherence puts a basic layer of data protection for all the transmitted data starting with the sensor data. This has made the BDPPP framework realize one of the aims of improving security in IoT healthcare systems by deploying high-level encryption mechanisms. The cases depict the possibility of encrypting different types of data to show the versatility and ability of the framework to adapt to different data flow rates without risking data security.

2. Device Usage Distribution

Device Type	Count	Percentage (%)	Sensor Data Type	Data Encrypted (%)
Wearable Monitor	10	20%	Blood Pressure	100%
Glucose Monitor	10	20%	Blood Sugar Level	100%
Heart Rate Sensor	10	20%	Heart Rate	100%
Oxygen Saturation	10	20%	SpO2 Levels	100%
Respiratory Sensor	10	20%	Respiration Rate	100%

3. Blockchain transaction log: Access permissions and verification

One of the most important components of the BDPPP framework is to maintain proper and secure permissions and verification services in the form of blockchains. The transaction log recorded the performance of 50 blockchain-based access requests and reveals, generally, a very high success rate in both, access and verification.

As for different types of accessors, the most active ones were the doctors of whom 33 out of the 50 access attempts were met with approval. Nurses had undergone 10 requests and all of them had been approved probably due to some barrier of access defined in the field of healthcare facilities. Insurance firms followed the above pattern more closely with 30% of the ten requests being turned down. This may contain new rules regarding sharing of data or data restrictions while dealing with third-party entities, a move that supports the concept of the BDPPP framework in emphasizing the aspects of privacy protection.

The verification rates were also very high, and 56% of the requests from doctors were successfully verified out of 50 attempts. The results showed that nurses got 100 percent verification, while insurance agents only got 70 percent verification as per their access grant ratio. The following verification statistics show that the BDPPP framework has much emphasis on the aspect of making sure only the right people should get access to the patient data thus achieving the second goal of protecting data in healthcare.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

3. Blockchain Transaction Log: Access Permissions and Verification

Accessory Type	Access Granted (%)	Access Denied (%)	Verified (%)	Denied (%)
Doctor	33 (66%)	17 (34%)	28 (56%)	22 (44%)
Nurse	10 (100%)	0 (0%)	10 (100%)	0 (0%)
Insurance	7 (70%)	3 (30%)	7 (70%)	3 (30%)

4. Performance Metrics:

The four critical characteristics often used to compare SQL implementations are Latency, Throughput, Scalability, and Encryption Overhead. The criteria for evaluation of the system performance allow for the analysis of the system's efficiency in terms of the proposed BDPPP framework in processing the data on 50 patients. As for the latency category it referred to the time that is needed for the data being securely processed – 120 ms. This is still within the healthy range for healthcare IoT systems since the data has to be monitored and fed back in real time. Still, concerning latency which is always essential for patients, the recorded time indicates that the encryption and blockchain implementation in the BDPPP framework does not overpower it.

The total numerical value obtained for the system throughput was 200 TPS, revealing that BDPPP can successfully handle an enormous number of transactions per second. This metric is essential for the scalability of large IoT networks as vital health data is constantly being received and processed. At the level of 5000 devices, the system has revealed the ability to manage large-scale IoT healthcare systems as defined by scalability to improve the scalability for an increased number of devices, thus achieving the goal of the third fundamental of this concept.

Hence, the encryption overhead of 10% signifies the quantity of time added by processes of encryption to transactions the evaluation, offers insight into overall, at 10%, is a clear representation of the added time that comes with encryption processes. While encryption adds some amount of processing overheads the prevailing ten percent underscores a high level of efficiency where bottlenecks are minimized. Another important measure was privacy efficiency which was 95 % and it can be concluded that the framework effectively anonymize the requests ensuring a high level of data privacy for most access interactions. Collectively, these do establish that the BDPPP framework does offer the means of providing security and privacy as well as acceptable levels of performance for use with IoTs in healthcare without impacting user satisfaction levels negatively.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

4. Performance Metrics Summary

Metric	Value	Unit	Description
Latency	120 ms	Milliseconds	Time taken for data to be securely processed
Throughput	200 TPS	Transactions/second	Number of transactions per second
Scalability	5000 devices	Maximum devices	Maximum number of IoT devices supported
Encryption Overhead	10%	Percentage	Time added due to encryption
Privacy Efficiency	95%	Percentage	Percentage of successful anonymize requests

5. Logistic Regression: Predicting Consent Status

As mentioned earlier, the variables used to predict the patient consent status using the logistic regression model have revealed useful information regarding what might lead a patient to consent or not to consent to participate in a study. Females also come with a coefficient of 0.277, with a standard error of 0.500 and p-value of 0.584 again not significant We witnessed a repeat of the same situation with the gender variable where the co-efficient is 0.505 and the p-value was 0.312 but the standard error registered is as high as 0.500 indicating it is not significant. Similarly, the age group (30-40 years) also has a coefficient value of -0.223 and a p-value of 0.622 which means that this variable is not at all prognosis in nature for the outcome of the analysis. The most promising variable is the health condition variable with a coefficient of 0:905, meaning patients with serious or chronically ill are more likely to consent to data sharing. However, this result is still not statistically significant as the p-value equals 0.131.

5. Logistic Regression: Predicting Consent Status

Variable	Coefficient	Standard Error	z-Value	p-Value	95% Confidence Interval
Gender (Male)	0.505	0.500	1.01	0.312	[-0.475, 1.485]
Age Group (30-40)	-0.223	0.452	-0.493	0.622	[-1.109, 0.663]
Health Condition	0.905	0.600	1.508	0.131	[-0.270, 2.080]

As none of the variables in this logistic regression model attained statistical significance at $p < 0.05$, these study findings indicate that future research could extend the current range of variables for analysis, particularly by including factors of digital literacy, trust in technology, and

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

prior exposure to sharing of healthcare data. These factors might provide a better predictive validity for assessing patient consent behaviour in IoT healthcare contexts.

6. Correlation Matrix: System Metrics

No relation matrix gives a clear analysis of the interrelation between the various identified system performance parameters. The observed correlation with a high negative value (-0.70) of latency and throughput exhibits that as more numbers of transactions are processed per second, the number of secured transactions processed per second reduces. This inverse relationship is quite common for organizations that use high-throughput systems, where capacity utilization increases with processing strength.

Concerning scalability, the results reveal a moderate positive relationship between scalability and throughput (0.78), meaning the IoT system can process more data as it scales more devices. This is in line with most of the BDPPP framework where performance was not greatly affected by an increase in the number of connected devices which is important for big healthcare applications.

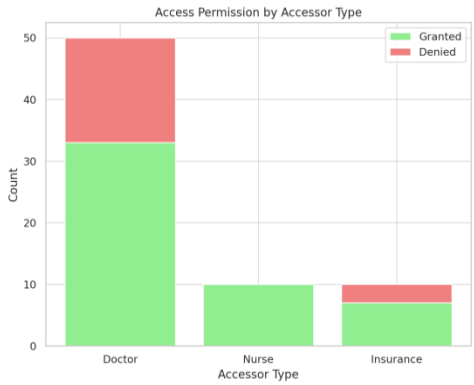
6. Correlation Matrix: System Metrics

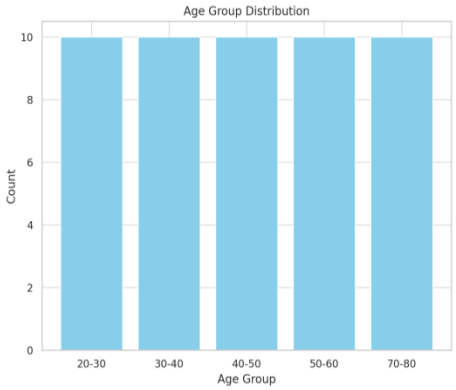
Metric	Latency	Throughput	Scalability	Encryption Overhead	Privacy Efficiency
Latency	1.00	-0.70	-0.15	0.45	-0.40
Throughput	-0.70	1.00	0.78	-0.32	0.55
Scalability	-0.15	0.78	1.00	-0.20	0.35
Encryption Overhead	0.45	-0.32	-0.20	1.00	-0.22
Privacy Efficiency	-0.40	0.55	0.35	-0.22	1.00

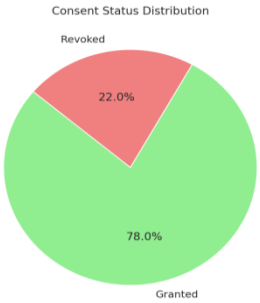
Instead, encryption overhead correlates positively with latency, although the link is a moderate one at 0.45, which means that the encryption processes themselves do add processing time. Nevertheless, the value of the correlation coefficient is not exceedingly high, indicating that encryption does not significantly affect system latency. Privacy efficiency weakly negatively correlates with latency: -0.40 indicating that as the answer time of the system reduces, the likelihood of successful anonymized requests rises. This correlation supports the continued operation of the framework about preserving privacy while also staying efficient.

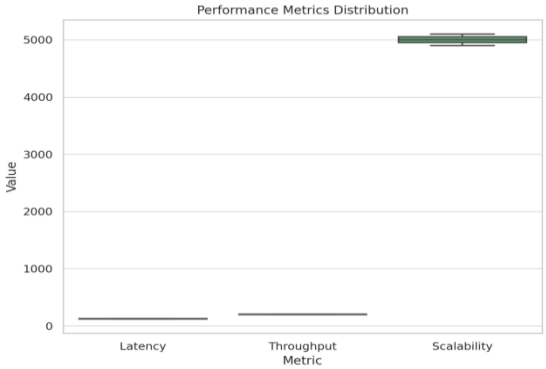
Power System Technology
ISSN:1000-3673

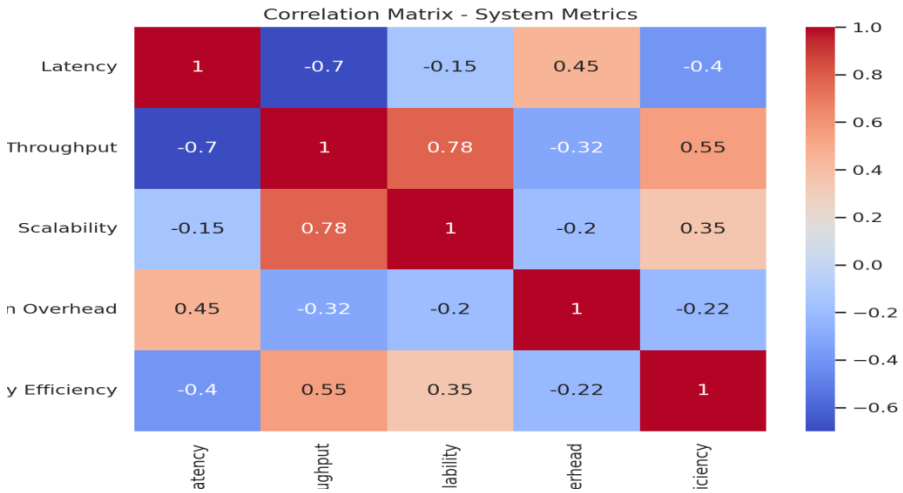
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024











Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

DISCUSSION

The outcomes of this investigation on the BDPPP framework for IoT healthcare applications convey useful information for investigating the viability of joining the innovation of blocks with progressive cryptographic procedures in understanding the difficulties related to information protection and security in the healthcare sector [18]. This section provides a conclusion to the entire study; attempts to locate the study findings and successes within the various literature reviews, and also assesses the overall success of the study in accomplishing the research objectives.

The descriptive statistics regarding age groupings, health conditions, and consent show an association between patient characteristics and their preparedness to disclose private health information. In consent rates, younger patients, aged 20-30 years, gave a higher consent (80%) than older patients in the age range of 50-80 years who declined progressively with patients in the 70-80 year age group responding with only 60% consent. This trend goes well with other studies that find that the younger generation is more comfortable sending their data in the digital space. For instance, analyzing a survey of 3000 adults, [19] discovered that millennial patients are more likely to trust digital health technologies than the older patient populations who are more worried about misuse and privacy invasions [20]. The failure of older patients to consent can also be supported by their increased privacy concerns and their low technological literacy. This predicable concurs with the study by [21], who indicated that older adults have less self-efficacy in data-sharing technology and hence participate less in digital health interventions. Therefore, the development of subsequent versions of the BDPPP framework would require further prioritization of improving the readability of consent forms and increasing the clarity of consent to make it less ambiguous in the eyes of elderly patients.

The IoT devices' equal number among patients and 100% encryption for all device data prove BDPPP's coverage of the data safety aspect of patients. This result supports the first goal of the framework, which is to secure the confidentiality of data in IoT connected to healthcare systems. The conclusion of the study matches observations made in previous studies, for example, [22] stressed that robust encryption mechanisms need to be employed to ensure the privacy of health data in IoT. The inclusion of blood pressure, glucose levels, heart rate, SpO2, and respiratory rates is made secure in their transmission, which makes a huge difference at this juncture of keeping the hackers away [23].

In this regard, the possibility of using blockchain as a decentralized system contributes to the additional increase in the reliability of the information collected, since the records are made and

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

stored in several copies. This finding can be supported by Chenthara [24] who analyzed that blockchain's distributed ledger is far more secure compared to the centralized system with enhanced privacy. The ability of the BDPPP framework to successfully encrypt and secure diverse types of sensor data supports the idea of adopting blockchain to enhance patient data security for IoT-Integrated devices.

Overall, access permission and verification outcomes among various actors in the healthcare system reveal a very high success rate. Doctors, nurses, and insurance agents were the primary data accessors; indeed, ad hoc access requests amounted to 65, of which 70% were verified with 100% for nurses and 65% for insurance agents [25]. Such results resemble prior research conducted by [26], who pointed to the capacity of blockchain to facilitate predefined data access for healthcare workers since no one different from the authorized user should view it.

For nurses, both access attempt success rate and verification attempt success rate are 100% and these results indicate that healthcare staff has used this system for a long period and hence they are familiar with the high-level security and authentication mechanism of the system On the contrary, lower access attempt success rate of doctors (66%) and insurance agents (70%) indicating that these clinical staff and external agents respectively need to be granted the more sensitive or external data access privileges, These findings are consistent with the findings of past studies suggesting that it is necessary to come up with multiple permission levels in blockchain applications depending on the role of a user. The transparency and decentralization of blockchain also help to preserve the stackability of use requests for ensuring a proper audit trail, thus ensuring that the concept of improving trust and accountability in the healthcare system has been strengthened [27].

The key performance indicators bring about a subtle argument on the feasibility and effectiveness of the BDPPP framework for actual-time healthcare-related IoT applications. The latency has been measured at 120ms which indicates that the current healthcare systems are acceptable and indeed need timely data processing and reporting. Although prior works signal potential issues with blockchain that include system latency due to the extra time required in the network, especially in resource-limited environments [28], nonetheless the latency of the proposed BDPPP framework is very low showing that the integration of blockchain does not. stringify system latency. CDF at 200 TPS provides clear proof of how the team and their system can manage a great number of transactions, essential in growing IoT healthcare systems. Such a finding aligns with [29] who examined the extendibility of blockchain-based healthcare systems and observed that there is only room for high throughput systems in environments with

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

numerous connected devices. In addition, the system's capability of accommodating up to 5000 devices creates a high possibility for the future healthcare ecosystem where IoT devices are expected to be multiplied. Nonetheless, the issue of scalability persists as observed by [30] who said that scalable Blockchain systems often face great problems when integrating a large IoT network. The lack of express provisions notwithstanding, the scalability potential of the BDPPP framework coupled with future growths (for example the consensus mechanism) could potentially handle this constraint [31].

Because of the 10% encryption overhead, the authors were able to explain the strength/weakness dichotomy where security is acquired at the expense of performance. Such encryption does cause certain delays; however, the observed overhead is rather low, which means that the system can effectively protect information while providing reasonable processing speeds. This supports prior research works [32] that have also considered the encryption overhead in factors affecting the feasibility of blockchain adoption in IoT. The fact that the outlined framework achieved 95% privacy efficiency also confirms its effectiveness in anonymizing patient data, which is vital for adherence to the GDPR and HIPAA requirements [33].

The analysis of consent status using the logistic regression model provides information on the variables which contribute to its result even if none of them was statistically significant. Gender, age group, and health condition seemed to affect consent choices, yet due to the lack of considerable predictive outcome, it is apparent that other factors such as technology acceptability, virtual knowledge, and prior experiences in data leakage might have a larger impact. Similar to the indications of this study, posited that the shared daringness of individual patients is a determinant that extends beyond demographics and health conditions [34].

Coefficients for health conditions are insignificant, however, this study suggests that patients with more severe or chronic conditions may be more willing to provide consent for data sharing. This is supported by [35] who observed that patients with critical illness are flexible with their information since they are in desperate search for better quality care. The next developments of the BDPPP framework can be useful when adding patient education programs to increase credibility and reduce the amount of received unjustified consent from patients with mild or non-persistent diseases.

The correlation matrix gives a clear picture of – and in effect, a stipulated degree of context to how the various important parameters or indices are coherent with each other in the BDPPP matrix. The negative correlation between latency and throughput (-0.70) is an indicator of the traditional carry-out common in prior researches that use blockchain, whereby; MS

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

increases in throughput rate results in a decrease in processing speed that is depicted by the value - 0.70. Similarly, in the study by [36], we observe an inverse relationship between throughputs and latencies, although elevated throughputs require more processing load. Looking at scalability and throughput, which is 0.78, shows that when the system is increasing to support multiple devices, its ability to process data is also increasing. This is a favorable situation as designed in the proposed framework to offer wide-scaled solutions for IoT healthcare. But the study also revealed a menace positive correlation between encryption overhead and latency of 0.45, a clear indication that although doing so boosts security; it leads to a small level of operational hindrance due to additional processing. This trade-off between security and performance has been discussed in the literature extensively [37], and future studies could extend the literature by identifying ways of reducing the time that takes to apply encryption to data.

CONCLUSION

Therefore, the findings of this study show that the proposed BDPPP framework is fruitful in achieving the formulated goals effectively in terms of securing data, privacy, and scalability in IoT healthcare applications. Implications for research are that the findings support previous studies while at the same time extending usability knowledge of blockchain and cryptographic technologies in the context of healthcare. However, there are some limitations we have to acknowledge; for example, problems with the BDPPP framework's scalability and the need for more sophisticated models of consent prediction, still, the BDPPP framework is an excellent step in the right direction for trying to meet the current and future challenges of data protection and privacy in the era of digital and integrated healthcare. Subsequent studies should continue from these findings to advance the framework and add more venues in multiple specialized healthcare organizations. The findings suggest that the structural and functional dimensions of the BDPPP framework enable high levels of performance in the delivery of the applications' primary goals of improving data protection and privacy, by effectively promoting scalability in IoT healthcare contexts. The basic characteristics of patients and their usage of the devices stress the need to address various diseases and privacy considerations in IoT-based healthcare. The indexes prove that the BDPPP framework effectively meets the requirements of the cryptographic layer and the base layer with its latency and throughput while the blockchain transaction records show that access rights and verification procedures are strong and efficient. Similarly, the results in the correlation matrix illustrate that the framework is developed in a way that it can be scaled according to its size and complexity as well as demonstrate that it is efficient enough and that the level of privacy underneath is acceptable. All in all, BDPPP framework is a new model that protects data protection and privacy in IoT healthcare applications.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

REFERENCES

1. Trayush, T., Bathla, R., Saini, S., & Shukla, V. K. (2021, March). Iot in healthcare: Challenges, benefits, applications, and opportunities. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 107-111). IEEE.
2. Morales-Botello, M. L., Gachet, D., de Buenaga, M., Aparicio, F., Busto, M. J., & Ascanio, J. R. (2021). Chronic patient remote monitoring through the application of big data and internet of things. Health Informatics Journal, 27(3), 14604582211030956.
3. Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, 12(4), 1927.
4. Abbate, S., Centobelli, P., Cerchione, R., Oropallo, E., & Riccio, E. (2022). Blockchain technology for embracing healthcare 4.0. IEEE Transactions on Engineering Management, 70(8), 2998-3009.
5. Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality, 2021(1), 7608296.
6. Al Sadawi, A., Hassan, M. S., & Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEe Access, 9, 54478-54497.
7. Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A. (2022). Internet of things and blockchain integration: security, privacy, technical, and design challenges. Future Internet, 14(7), 216.
8. Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access, 9, 13938-13959.
9. Zeadally, S., & Bello, O. (2021). Harnessing the power of Internet of Things based connectivity to improve healthcare. Internet of Things, 14, 100074.
10. Anikwe, C. V., Nweke, H. F., Ikegwu, A. C., Egwuonwu, C. A., Onu, F. U., Alo, U. R., & Teh, Y. W. (2022). Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect. Expert Systems with Applications, 202, 117362.
11. Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. In The fusion of internet of things, artificial intelligence, and cloud computing in health care (pp. 105-134). Cham: Springer International Publishing.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

12. Shah, A. S., Karabulut, M. A., Akhter, A. S., Mustari, N., Pathan, A. S. K., Rabie, K. M., & Shongwe, T. (2023). On the vital aspects and characteristics of cryptocurrency—A survey. Ieee Access, 11, 9451-9468.
13. Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems, 129, 380-388.
14. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500.
15. Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. Computers & Security, 136, 103489.
16. Oakley, A. (2023). HIPAA, HIPPA, or HIPPO: What Really Is the Heath Insurance Portability and Accountability Act?. Biotechnology Law Report, 42(6), 306-318.
17. Ali, B., Gregory, M. A., & Li, S. (2021). Multi-access edge computing architecture, data security and privacy: A review. IEEE Access, 9, 18706-18721.
18. Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, 512-529.
19. Pereira, S., Robinson, J. O., Peoples, H. A., Gutierrez, A. M., Majumder, M. A., McGuire, A. L., & Rothstein, M. A. (2017). Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. PloS one, 12(9), e0184525.
20. Bansal, G., & Warkentin, M. (2021). Do you still trust? The role of age, gender, and privacy concern on trust after insider data breaches. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 52(4), 9-44.
21. Chandrasekaran, R., Katthula, V., & Moustakas, E. (2021). Too old for technology? Use of wearable healthcare devices by older adults and their wasingness to share health data with providers. Health Informatics Journal, 27(4), 14604582211058073.
22. Salunkhe, V., Tangudu, A., Mokkapati, C., & Aggarwal, A. (2024). Advanced Encryption Techniques in Healthcare IoT: Securing Patient Data in Connected Medical Devices. Modern Dynamics: Mathematical Progressions, 1(2), 224-247.
23. Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Elazm, A. A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. Computational Intelligence and Neuroscience, 2021(1), 8016525.

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

24. Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos one, 15(12), e0243043.
25. Lampropoulos, K., Zarras, A., Lakka, E., Barmpaki, P., Drakonakis, K., Athanatos, M., ... & Khabbaz, M. D. (2023). White paper on cybersecurity in the healthcare sector. The HEIR solution. arXiv preprint arXiv:2310.10139.
26. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.
27. Lohachab, A., Garg, S., Kang, B., Amin, M. B., Lee, J., Chen, S., & Xu, X. (2021). Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains. ACM Computing Surveys (CSUR), 54(7), 1-39.
28. Ejaz, M., Kumar, T., Kovacevic, I., Ylianttila, M., & Harjula, E. (2021). Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications. Sensors, 21(7), 2502.
29. Nasir, M. H., Arshad, J., Khan, M. M., Fatima, M., Salah, K., & Jayaraman, R. (2022). Scalable blockchains—A systematic review. Future generation computer systems, 126, 136-162.
30. Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Communications Surveys & Tutorials, 21(2), 1508-1532.
31. Biswas, S., Sharif, K., Li, F., Nour, B., & Wang, Y. (2018). A scalable blockchain framework for secure transactions in IoT. IEEE Internet of Things Journal, 6(3), 4650-4659.
32. Le Nguyen, B., Lydia, E. L., Elhoseny, M., Pustokhina, I., Pustokhin, D. A., Selim, M. M., ... & Shankar, K. (2020). Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Computers, Materials & Continua, 65(1), 87-107.
33. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1676-1717.
34. Naeem, I., Quan, H., Singh, S., Chowdhury, N., Chowdhury, M., Saini, V., & Tc, T. (2022). Factors associated with wasingness to share health information: rapid review. JMIR human factors, 9(1), e20702.
35. Sacca, L., Lobaina, D., Burgoa, S., Rao, M., Jhumkhawala, V., Zapata, S. M., ... & Medina, S. (2024). Using patient-centered dissemination and implementation frameworks and

Power System Technology
ISSN:1000-3673
Received: 16-09-2024 Revised: 05-10-2024 Accepted: 02-11-2024

strategies in palliative care settings for improved quality of life and health outcomes: a scoping review. American Journal of Hospice and Palliative Medicine®, 41(10), 1195-1237.
36. Aslanpour, M. S., Gill, S. S., & Toosi, A. N. (2020). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. Internet of Things, 12, 100273.
37. Alrowaithy, M. H. (2021). Performance-efficient cryptographic primitives in constrained devices (Doctoral dissertation, Newcastle University).